Безопасная разработка на службе ИБ

Иван Румянцев
Ростелеком

Что мы узнали внедряя SSDLC

Отношение разработчиков к безопасности

Отношение разработчиков к безопасности

Для команды разработки исправление уязвимостей:

- Не представляет ценности
- Придется отодвинуть бизнес задачи, отдав приоритет ИБ

Так не всегда!

Есть команды внимательно относящиеся к безопасности. Обычно это:

- Зрелые команды
- Хорошо автоматизированные процессы

Дайте денег

- Стоимость исправления всех уязвимсостей высока
- Не всегда есть бюджет, выделенный на работы по ИБ

Подрядчики не беспокоятся о безопасности. Совсем.

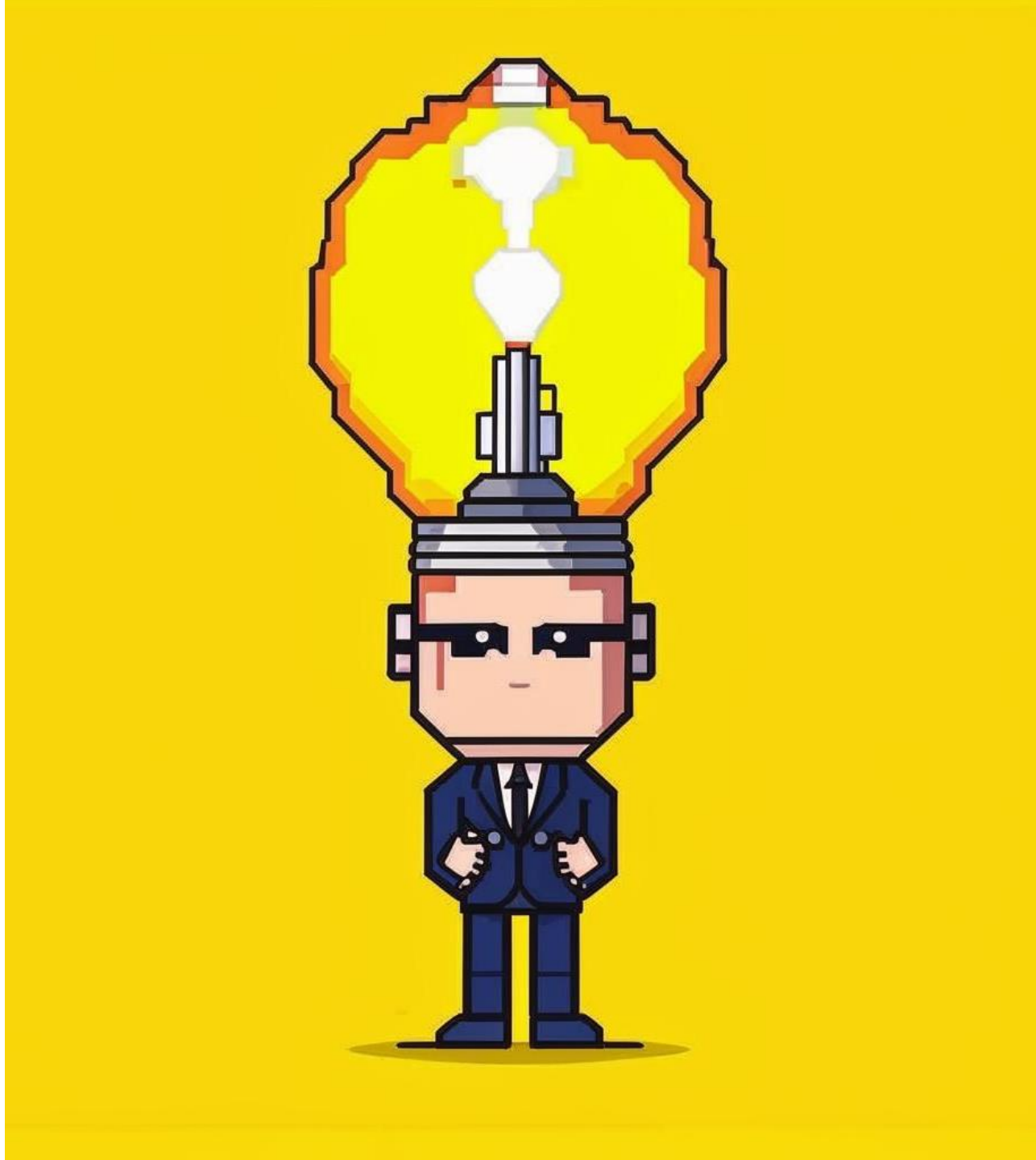
- Подрядчику важнее разработать бизнес функционал
- Подрядчик чаще не готов делиться исходным кодом
- Исправление уязвимостей повышает стоимость разработки

Еще проблемы

Еще проблемы

- Большое количество уявзимостей обнаруженных инструментами
- Отсутствие возможности быстро исправить уязвимости
- Баланс между TTM и безопасностью

Что мы сделали для повышения культуры ИБ

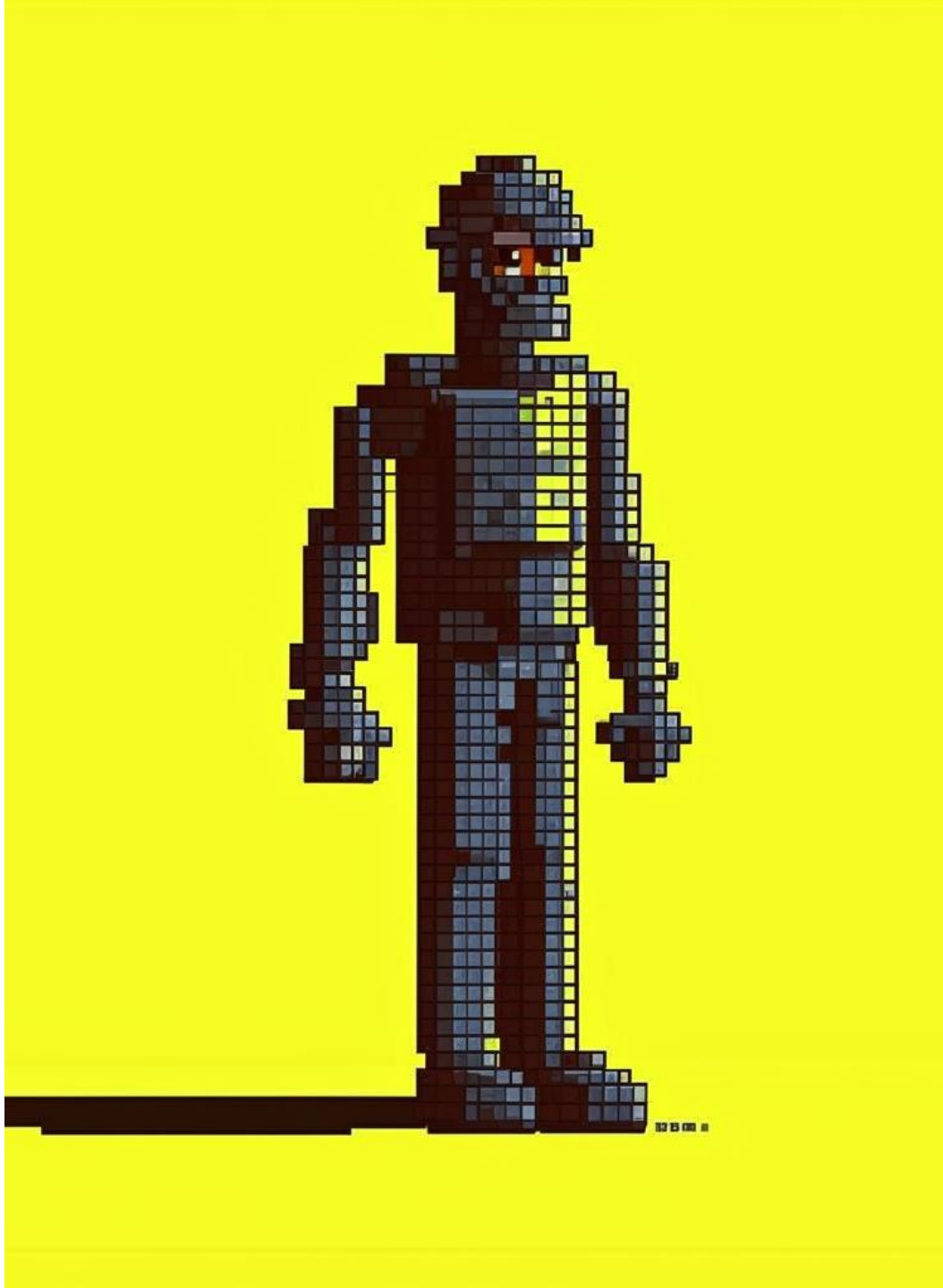


Сформировать у разработчиков понимание что такое уязвимости

- Проведение общих семинаров по безопасности
- Организация внутренних CTF для разработчиков, DevOps, инженеров
- Создание каналов для общения и вопросов с Блоком ИБ

Найти людей которым интересна ИБ

- Учредили институт Security Champion
- Участники CTF
- Команды, самостоятельно внедряющие у себя инструменты безопасности



Решения

Уязвимост

Приоритезация

- Начать с самых распространенных практик
- Смотреть сверху вниз от критичных до низких

Уязвимост -18%

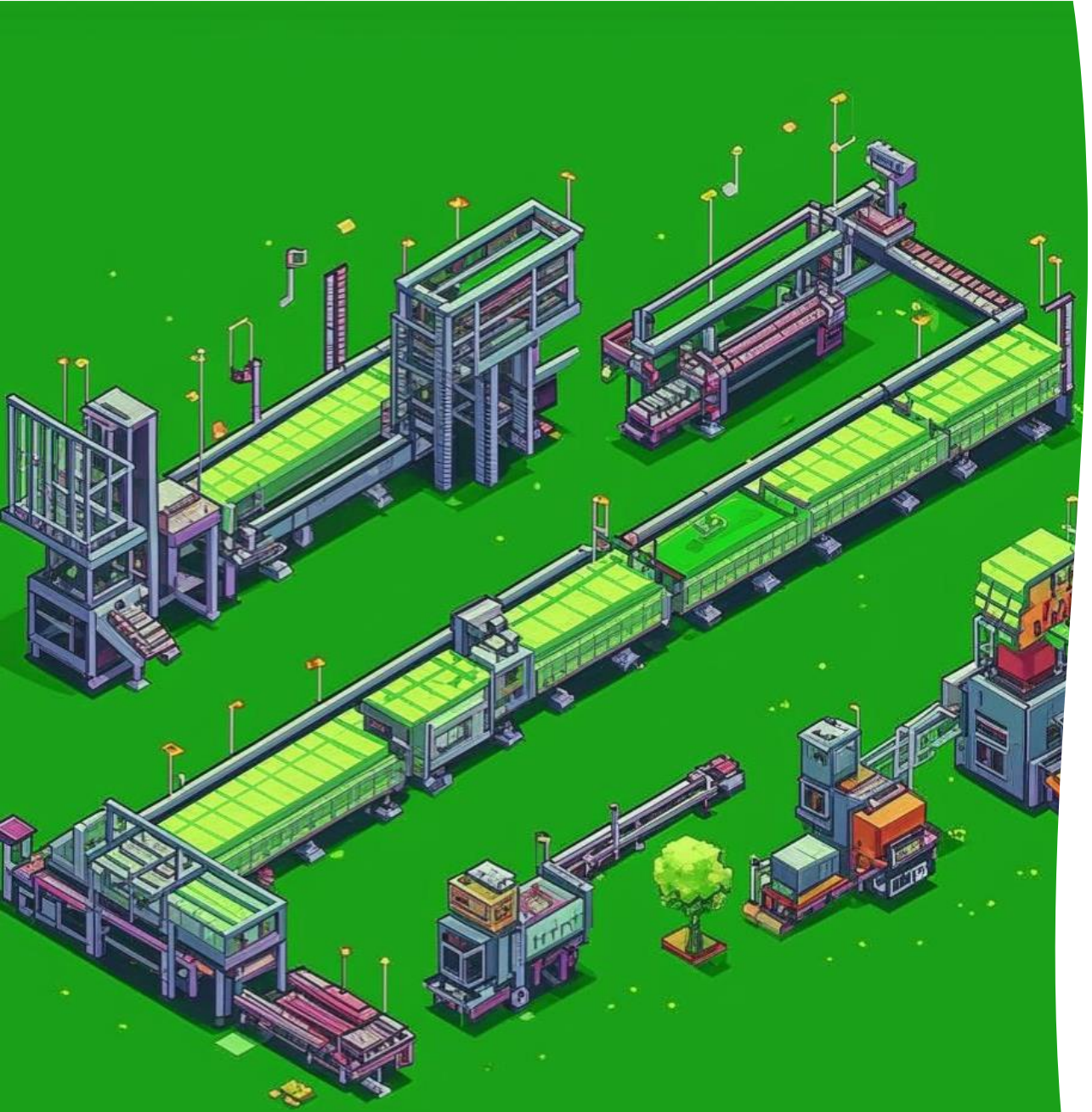
Приоритизация

- ✓ Начать с самых распространенных практик
- Смотреть сверху вниз от критичных до низких

Уязвимост -36%

Приоритизация

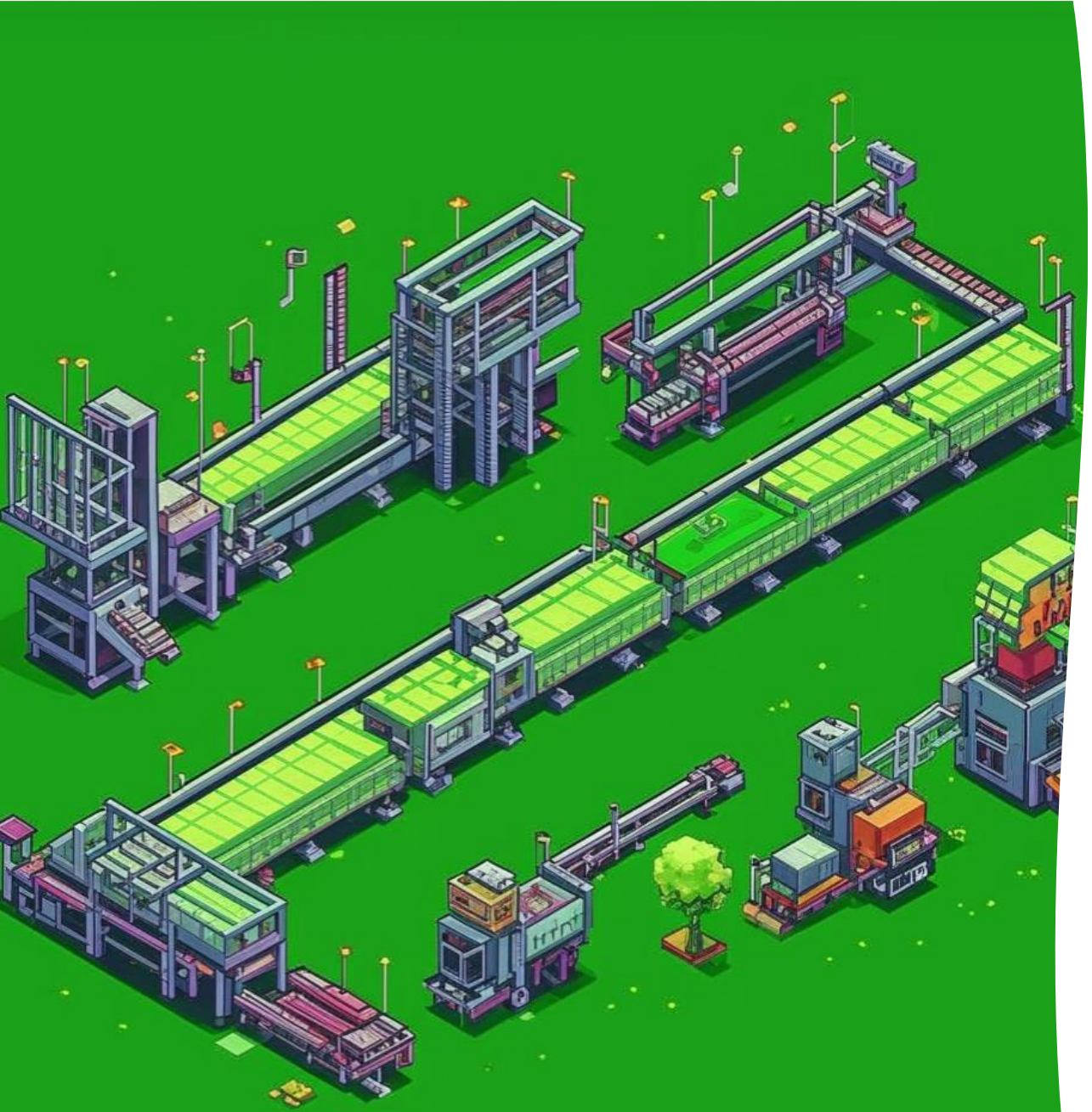
- ✓ Начать с самых распространенных практик
- ✓ Смотреть сверху вниз от критичных до низких



Уязвимост

Автоматизация и тюнинг

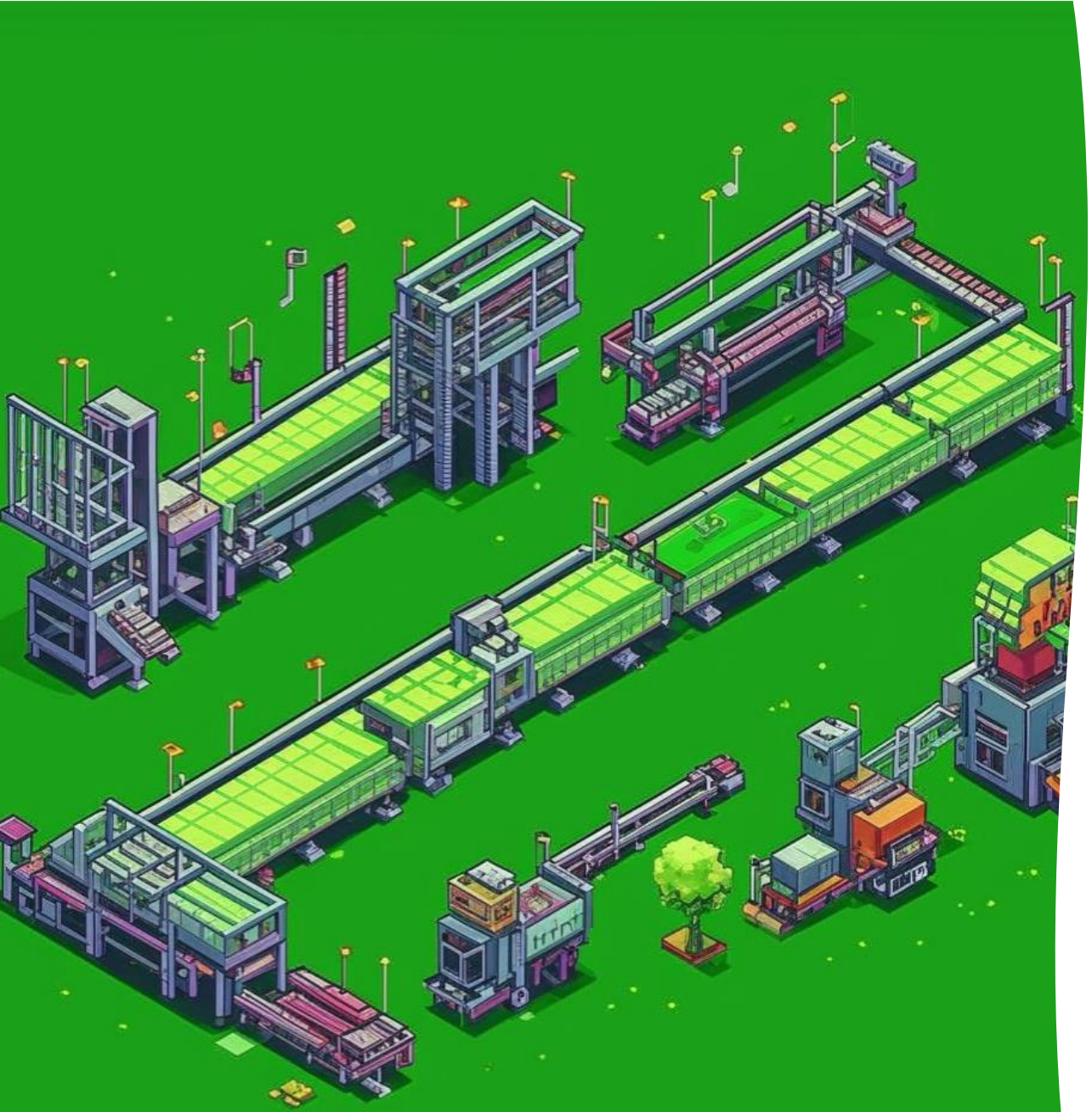
- Не разбирать то что с большой долей вероятности является истинной
- Подключать ML/AI
- Дорабатывать инструменты, писать правила. Снижать количество False Positive



Уязвимост -4%

Автоматизация и тюнинг

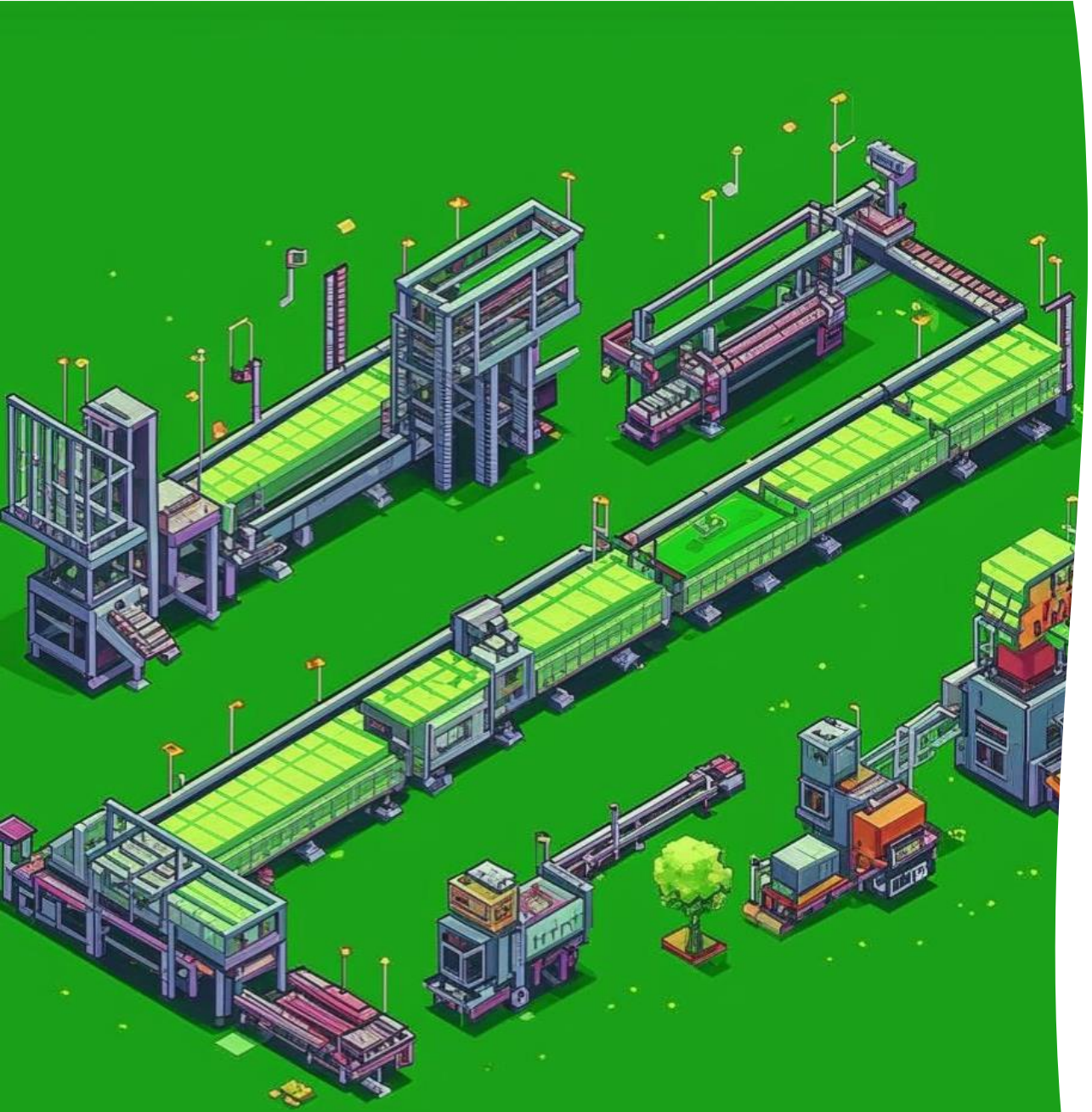
- ✓ Не разбирать то что с большой долей вероятности является истинной
- Подключать ML/AI
- Дорабатывать инструменты, писать правила. Снижать количество False Positive



Уязвимост -1%

Автоматизация и тюнинг

- ✓ Не разбирать то что с большой долей вероятности является истинной
- ✓ Подключать ML/AI
- • Дорабатывать инструменты, писать правила. Снижать количество False Positive



Уязвимост -3%

Автоматизация и тюнинг

- ✓ Не разбирать то что с большой долей вероятности является истинной
- ✓ Подключать ML/AI
- ✓ Дорабатывать инструменты, писать правила. Снижать количество False Positive

Оптимизация процесса

- Shift-left – чем быстрее получена информация о уязвимости, тем меньше ресурсов нужно чтоб ее исправить.
- Подключать разработчиков к триажу. False Positive дошедшей до разработчика, не так страшен как ошибочно отброшенный True Positive

Больше требований. И возможность их обойти

- Требовать от подрядчиков минимальных мер ИБ
- Security Gate, хотя бы в уведомительном режиме
- Возможность зрелым командам самостоятельно строить процессы безопасной разработки. Под нашим контролем.

Подключать внешних и внутренних исследователей

- Багбаунти, хотя бы внутренний
- Проводить периодические пентесты приложений. Сравнивать результаты, с результатами SSDLC

(Не)очевидные выгоды

Безопасность – конкурентное преимущество

- Крупные компании требуют наличия безопасной разработки при заключении контракта

- Чем продукт безопаснее, тем выгоднее он смотрится на рынке

Репутационные потери – не миф

• Информация о сливах и взломах распространяется очень быстро, что наносит ущерб репутации компании

Спасибо!

pr@rt.ru